Especificación y Verificación Formal de Sistemas Críticos

Análisis de Modelos de Seguridad para Dispositivos Móviles

Carlos Luna[♣♦], Gustavo Betarte[♦]

[♣] Departamento de Ciencias de la Computación. Facultad de Ciencias Exactas, Ingeniería y Agrimensura.

Universidad Nacional de Rosario. Rosario, Argentina.

[♦] Instituto de Computación. Facultad de Ingeniería. Universidad de la República. Montevideo, Uruguay.

{cluna,gustun}@fing.edu.uy

Resumen— Este documento presenta resultados generados principalmente en el marco de una línea de investigación que involucra a dos proyectos de investigación: "Especificación formal y verificación de sistemas críticos", SeCyT-FCEIA, UNR (ING266), Argentina; y "STEVE: Seguridad a Través de Evidencia VErificable", proyecto PDT, DINACYT, Uruguay. Asimismo, algunas actividades de estos proyectos se enmarcaron en un proyecto de cooperación STIC-AMSUD: "ReSeCo: Reliability and Security of Distributed Software Components". El artículo describe esencial y sucintamente los trabajos realizados, las principales publicaciones obtenidas y la formación de recursos humanos en Argentina y Uruguay.

Palabras clave: *escificación formal, sistemas críticos, modelos de seguridad para dispositivos móviles (MIDP), asistentes de prueba (Coq).*

1. INTRODUCCIÓN

Este documento presenta resultados generados principalmente en el marco de una línea de investigación que involucra a dos proyectos de investigación: *Especificación formal y verificación de sistemas críticos*, SeCyT-FCEIA, UNR (ING266), Argentina [1]; y *STEVE: Seguridad a Través de Evidencia VErificable*, proyecto PDT, DINACYT, Uruguay [2]. Asimismo, algunas actividades de estos proyectos se enmarcaron en un proyecto más general de cooperación STIC-AMSUD: *ReSeCo* (*Reliability and Security of Distributed Software Components*) [3].

La organización del documento es como sigue. La sección 2 describe los proyectos en los cuales se enmarca la investigación desarrollada. La sección 3 presenta los principales resultados obtenidos en una de las líneas de investigación contempladas por los proyectos descritos en la sección 2. Luego, la sección 4 aborda la formación de recursos humanos de grado y postgrado, tanto en Argentina como en Uruguay, en el contexto de los proyectos referidos. Finalmente, la sección 5 analiza los próximos pasos a seguir en esta investigación.

2. CONTEXTO

2.1 ReSeCo: Reliability and Security of Distributed Software Components

El proyecto STIC-AMSUD (www.sticamsud.org) *ReSeCo* ha tenido como principal objetivo investigar la seguridad y fiabilidad en un modelo computacional, donde tanto las plataformas como las aplicaciones son dinámicas, de forma que componentes provistos por un agente externo puedan ser destinados a formar parte de la plataforma o ejecutar una aplicación de forma segura. El proyecto buscó además incentivar la colaboración entre la comunidad científica, e industrial, de Francia y de países Sudamericanos.

Dentro de los objetivos específicos que fueron definidos para este proyecto destacamos uno en particular: investigar la seguridad y fiabilidad en un modelo computacional, donde tanto las plataformas como las aplicaciones son dinámicas, de forma que componentes provistos por un agente externo puedan ser destinados a formar parte de la plataforma o ejecutar una aplicación de forma segura.

La contribución por parte de miembros del Instituto de Computación (InCo) de la Facultad de Ingeniería de la Universidad de la República (Uruguay) –con el apoyo de docentes y estudiantes del Departamento de Ciencias de Computación (DCC) de la Facultad de Ciencias Exactas, Ingeniería y Agrimensura de la UNR (Argentina)– al proyecto ReSeCo fueron principalmente desarrolladas en el contexto del proyecto STEVE, que es descrito a continuación. A modo de resumen, en relación al objetivo previamente referido de ReSeCo se trabajó en la especificación formal y la verificación de componentes críticos de la plataforma JME [4], una tecnología Java específica para dispositivos móviles.

El Dr. Gustavo Betarte fue el coordinador del proyecto por parte del Equipo Uruguayo.

2.2. STEVE: Seguridad a Través de Evidencia Verificable

El proyecto *STEVE* ha sido concebido en el marco del proyecto de cooperación ReSeCo descrito arriba. STEVE permitió elaborar y concebir mecanismos que ayudan a los desarrolladores de software a construir sistemas confiables a partir de componentes existentes, así como infraestructuras que garantizan al usuario final que el software que éste utiliza es seguro y confiable.

STEVE tuvo financiación de la DINACYT, Uruguay (programa PDT), se desarrolló bajo la dirección del Dr. Gustavo Betarte (InCo) y contó con la participación de docentes y estudiantes de Argentina (del DCC) y de Uruguay (InCo).

2.3. Especificación Formal y Verificación de Sistemas Críticos

El proyecto *Especificación Formal y Verificación de Sistemas Críticos* aspira a fortalecer un área de trabajo importante para el desarrollo de la informática en Argentina y en la región: el empleo de métodos formales en el ciclo de vida de software crítico. El principal objetivo es conformar un grupo estable de jóvenes investigadores en el área a través del estudio de problemas específicos de interés.

Este proyecto fue aprobado por la SeCyT-FCEIA, UNR, Argentina. Su código es ING266 y el responsable es el MsC Carlos Luna.

3. Línea de Investigación y Resultados Obtenidos

A continuación describimos brevemente una de las principales líneas de investigación enmarcadas, fundamentalmente, en el proyecto STEVE, e incluimos los principales resultados obtenidos.

Especificación y Verificación Formal de Modelos de Seguridad para Dispositivos Móviles

Los dispositivos portátiles, tales como teléfonos celulares y asistentes de datos personales, permiten almacenar información confidencial y establecer comunicaciones con entidades externas. Generalmente, los usuarios pueden descargar e instalar nuevas aplicaciones de fuentes no confiables, que conviven junto con las instaladas por el fabricante del dispositivo o proveedor de servicios de comunicación. En este escenario, es importante garantizar la confidencialidad e integridad de los datos almacenados, así como la disponibilidad del servicio, aún cuando una aplicación maliciosa trate de hacer uso indebido de las funciones del dispositivo. La plataforma Java Micro Edition (JME) [4], una tecnología para desarrollo de software Java, provee el estándar Mobile Information Device Profile (MIDP) [5,6,7] que facilita el desarrollo de aplicaciones y especifica un modelo de seguridad para el acceso controlado a recursos sensibles del dispositivo. El modelo está construido sobre la noción de dominio de protección, que puede ser concebido como un conjunto de permisos.

Un modelo alternativo que extiende los permisos presentes en MIDP ha sido propuesto por Besson, Dufay y Jensen [8]. Este modelo introduce una noción de multiplicidad asociada a los permisos y flexibiliza la forma en la que el usuario puede conceder acceso a los recursos del dispositivo, a las aplicaciones que son utilizadas en el mismo.

En el contexto del proyecto STEVE se trabajó en la especificación, en el cálculo de construcciones inductivas [9], y la verificación formal, usando el asistente de pruebas Coq [10], de componentes de modelos de seguridad para dispositivos móviles interactivos. En particular, se analizaron las tres generaciones de MIDP y se desarrolló un framework, en [11], que permite definir y comparar formalmente políticas de control de acceso, que pueden ser aplicadas por variantes de los modelos de seguridad considerados. En [12] desarrollamos una especificación general del modelo de seguridad de MIDP 2.0 [6], y en [13] implementamos un algoritmo de control de accesos, que certificamos respecto al comportamiento esperado del módulo correspondiente en MIDP 2.0.

El artículo [14] reporta la extensión del análisis formal a la reciente introducción de MIDP 3.0 [7], haciendo especial énfasis en el modelo de seguridad a nivel de aplicación que se incorpora sobre el modelo de seguridad a nivel de plataforma, ya existente en MIDP 2.0. En [15] desarrollamos algoritmos críticos certificados para nuevas funcionalidades de MIDP 3.0 y reportamos algunas vulnerabilidades de seguridad de la más reciente generación de MIDP, junto con propuestas de soluciones. Los diferentes prototipos certificados construidos podrán ser usados como implementaciones de referencia para, por ejemplo, desarrollar casos de prueba para las implementaciones industriales que se utilicen.

4 Formación de Recursos Humanos

En esta sección describimos brevemente las actividades de formación de recursos humanos. Inicialmente presentamos un curso que se desarrolla, desde hace varios años, tanto en Uruguay (en el InCo) como en Argentina (en el DCC). Luego mencionamos actividades de formación en el marco de proyectos de final de carrera (de grado, esencialmente).

4.1. Taller de Producción de Programas sin Fallas

El Taller de Producción de Programas sin Fallas (TPPSF) es un curso que se desarrolla en modalidad de taller para apoyar la enseñanza de métodos formales en una currícula de grado (y de postgrado), usando el asistente de pruebas *Coq* y conceptos del área de Teoría de Tipos. El taller abarca fundamentalmente la especificación, derivación y verificación de sistemas en diferentes paradigmas de programación. Debido a la característica de taller, el enfoque seguido es eminentemente práctico, orientado al análisis de aplicaciones, con un

fundamente teórico mínimo. Esta característica sumada a la utilización de herramientas de apoyo permiten una introducción al estudio formal de los temas abracados por el taller a estudiantes de distintas disciplinas de la informática e incluso de otras áreas, como la matemática.

4.1.1 Objetivos del TPPSF

- Presentar a la Teoría de Tipos como lógica de programación y familiarizar al estudiante con ambientes de desarrollo de programas basados en este formalismo.
- Iniciar al estudiante en el uso de métodos formales para la especificación, producción, derivación y verificación de software correcto por construcción en paradigmas tradicionales de programación, como el funcional.
- Iniciar al alumno en el uso de métodos formales para la especificación y verificación de otras clases de sistemas. En particular, sistemas críticos (sistemas reactivos y de tiempo real, y distintos modelos de seguridad).
- Mostrar la utilidad de editores de pruebas basados en teoría de tipos para la especificación y verificación de aplicaciones industriales y académicas.

La bibliografía usada en el taller incluye artículos del área de teoría de tipos y, fundamentalmente, manuales y tutoriales de la herramienta *Coq* [10, 16, 17], como así también el libro [9]. Información adicional sobre el curso y los materiales usados pueden consultarse en el sitio web "http://www.fing.edu.uy/inco/grupos/mf/TPPSF/". Asimismo, información acerca del proyecto *Coq* puede obtenerse en "http://*Coq*.inria.fr/".

4.1.2 Experiencias en el Desarrollo del Taller

El taller viene desarrollándose regularmente en el InCo desde el año 2000, en versiones ligeramente diferentes, tanto como curso de grado para la carrera de Ingeniería en Computación, como curso de postgrado para la Maestría o el Doctorado en Computación. Las primeras ediciones no abarcaban el estudio de sistemas críticos ni el análisis de aplicaciones industriales y académicas realizadas con *Coq*. Posteriores versiones fueron incorporando estas características y recientemente anexamos al taller un módulo para la especificación y el análisis de aplicaciones industriales (y académicas) con *Coq*. De esta manera logramos captar el interés, por estos temas, de estudiantes de áreas no directamente vinculadas con métodos formales.

En el año 2001 desarrollamos el taller en el Departamento de Computación de la FI de la UNRC (Río IV, Argentina), y en los años 2000, 2001 y 2005-2010 en el DCC de la UNR (Argentina). Asimismo, versiones cortas del taller se llevaron a cabo en las siguientes escuelas de ciencias informáticas: Rio'2000, desarrollada en Febrero de 2000, UNRC; y, ECI'2001, desarrollada en Julio de 2001, UBA, Bs. As., Argentina. Finalmente en Febrero de 2004 presentamos una versión del taller orientada a aplicaciones computacionales –industriales– de la demostración asistida de teoremas usando *Coq* en el marco de la Rio'2004, UNRC. Aplicaciones de este tipo son por ejemplo: protocolos de comunicación, compiladores, protocolos de comercio electrónico, sistemas operativos y aplicaciones seguras para tarjetas inteligentes y dispositivos móviles, entre otras.

En total, más de 400 estudiantes participaron de alguna edición del taller; tanto estudiantes del área de métodos formales como estudiantes de otras áreas de informática o de matemáticas, de grado y de postgrado. Los intereses en cada caso han sido diferentes y en este sentido los proyectos finales que se propusieron. A partir de estas experiencias surgieron varias tesis de maestría y tesinas (proyectos) de grado. Desde el año 2000 a la actualidad un número importante de proyectos de investigación han sido llevados a cabo. Asimismo, dos proyectos adicionales están en curso en el InCo en temas relacionados y varias colaboraciones con instituciones regionales e internacionales han sido establecidas, por ejemplo en el marco de proyectos STIC-AMSUD como *ReSeCo* y *FMCrypto*, o el proyecto CYTED *REVVIS*. El taller ha oficiado como punto de encuentro entre distintas áreas y nos ha permitido acercar a estudiantes con diferentes perfiles en una introducción "práctica" a los métodos formales, focalizándonos en la especificación, construcción y verificación de sistemas en diferentes paradigmas de programación.

Luego de las múltiples experiencias en el desarrollo del taller evaluamos altamente positivos los logros alcanzados. En particular, consideramos que los estudiantes de grado de una carrera de informática ven complementada su formación, dentro del área de métodos formales, con el taller propuesto. El taller les permite profundizar en la aplicación de técnicas de inducción-recursión y deducción en la definición y verificación de sistemas, como así también en la formulación y el análisis de especificaciones. Estos conceptos, que son centrales en la formación de profesionales universitarios en el área, consideramos que, al margen del aporte técnico que les representa, los entrena y capacita para una adecuación rápida y eficaz a los acelerados cambios tecnológicos, que son una constante en la disciplina.

4.2. Proyectos de Grado

Si bien la realización proyectos de grado se mencionó en la sección previa, concretamente en el marco de las líneas de investigación referidas en este artículo, varios proyectos de grado en Argentina (tesinas de Licenciatura) y en Uruguay (proyectos de Ingeniería) han sido llevados a cabo. Desde el DCC de la UNR participaron, entre otros: Santiago Zanella [12], Ramin Rosuhani [13] y Juan Manuel Crespo [11]. Asimismo, Cristian Rosa [19] y Dante Zanarini [20] trabajaron en formalizaciones, en el marco del proyecto ING266, aunque no relacionadas con dispositivos móviles. Actualmente José Forte, Ezequiel Bazán y Mauricio Chimento están realizando sus tesinas de Licenciatura en temas afines.

Por otra parte, el trabajo en Uruguay no sólo contempló la realización de trabajos de grado de la carrera de Ingeniería en Computación, sino que actualmente se está desarrollando una tesis de maestría en temas afines. Por más información sugerimos ver [2].

5. TRABAJO FUTURO

En el área de especificación y verificación de modelos de seguridad para dispositivos móviles, el objetivo en el corto plazo es profundizar el análisis de características novedosas de la última generación de MIDP (MIDP 3.0, aún no vigente), tales como: concurrencia, comunicación entre aplicaciones y almacenamiento de datos compartidos. Probar propiedades de *isolation* en este escenario es un objetivo importante. Para ello consideramos relevante tener en cuenta, en particular, resultados obtenidos recientemente por investigadores vinculados al equipo, como por ejemplo [18].

REFERENCIAS

[1] Project ReSeCo: Reliability and Security of Distributed Software Components. http://www-sop.inria.fr/oasis/reseco/, 2006-2009.

[2] Proyecto STEVE: Seguridad a Través de Evidencia VErificable. http://www.fing.edu.uy/inco/grupos/gsi/proyectos/index.php 2007-2009.

[3] Proyecto *Especificación Formal y Verificación de Sistemas,* SeCyT-FCEIA, UNR (Argentina). Código ING266, 2009-2011.

[4] Sun Microsystems, Inc.: Java Platform Micro Edition. http://java.sun.com/javame/index.jsp

[5] JSR 37 Expert Group: Mobile Information Device Profile for Java Micro Edition. Version 1.0. Sun Microsystems Inc., 2000.

[6] JSR 118 Expert Group. Mobile Information Device Profile for Java Micro Edition. Version 2.0. Sun Microsystems Inc. and Motorola Inc., 2002.

[7] JSR 271 Expert Group. Mobile Information Device Profile for Java Micro Edition.Version 3.0, Public Review Specification, Motorola Inc., 2008.

[8] Besson, F., G. Duffay and T. Jensen: A Formal Model of Access Control for Mobile Interactive Devices. En 11th European Symposium on Research in Computer Security (ESORICS'06), LNCS 4189, páginas 110-126, 2006.

[9] Bertot, Y. and P. Castéran: Interactive Theorem Proving and Program Development. Coq'Art: The Calculus of Inductive Constructions. Texts in Theoretical Computer Science. Springer-Verlag, 2004. http://www.labri.fr/publications/l3a/2004/BC04

[10] The Coq Development Team: The Coq Proof Assistant Reference Manual - Version V8.2, 2009. http://coq.inria.fr

[11] Crespo, J., G. Betarte and C. Luna: A Framework for the Analysis of Access Control Models for Interactive Mobile Devices TYPES. En al, S. Berardi et (editor): Types for Proofs and Programs 2008, volumen 5497 de Lectures Notes in Computer Science, páginas 49-63. Springer-Verlag, January 2009.

[12] Zanella, S., G. Betarte and C. Luna: A Formal Specification of the MIDP 2.0 Security Model. En Formal Aspects in Security and Trust, Fourth International Workshop, FAST 2006, Hamilton, Ontario, Canada, August 26-27, 2006, Revised Selected Papers, volumen 4691 de LNCS, páginas 220-234. Springer-Verlag, 2006.

[13] Roushani, R., G. Betarte and C. Luna: A Certified Access Controller for JME-MIDP 2.0 enabled Mobile Devices. En XXVIII International Conference of the Chilean Computer Science Society, IEEE CS Press, 2010.

[14] Mazeikis, G., G. Betarte and C. Luna: Formal Specification and Analysis of the MIDP 3.0 Security Model. En XXVIII International Conference of the Chilean Computer Science Society, IEEE CS Press, 2010.

[15] Mazeikis, G. y C. Luna: Autorización de Acceso en MIDP 3.0. En V Congreso Iberoamericano de Seguridad Informática, CIBSI'09, Noviembre 2009.

[16] Giménez, E. and Casteran, P. A Tutorial on [Co-]Inductive Types in Coq, *Technical Report INRIA*, 2005.

[17] Huet, G., Kahn, G. and Paulin-Mohring, C. The Coq Proof Assistant: A Tutorial, accesible en http://Coq.inria.fr/, 2004.

[18] G. Barthe, G. Betarte, J. D. Campo and C. Luna. Formally verifying isolation and availability in an idealized model of virtualization. Formal Methods 2011: 17th International Symposium on Formal Methods, Ireland. LNCS, to appear (2011).

[19] Luna, C., Rosa, C. Análisis Formal del Estándar NIST para modelos RBAC, Congreso Iberoamericano de Seguridad Informática, CIBSI'09, Uruguay, Noviembre de 2009.

[20] Zanarini, D. Especificación de Lógica Temporal Alternante en el Cálculo de Construcciones Coinductivas. Tesis de Licenciatura en Ciencias de la Computación, FCEIA, UNR, Argentina, 2008. http://www.fceia.unr.edu.ar/~ dante/thesis/main.pdf